



专题: 5G

面向 5G 雾计算中基于 Q-learning 的安全中继节点选择方法

涂山山^{1,2}, 于金亮^{1,2}, 孟远^{1,2}, WAQAS M³, 刘雷⁴

(1. 北京工业大学信息学部, 北京 100124; 2. 可信计算北京市重点实验室, 北京 100124;
3. 清华大学电子工程系, 北京 100084; 4. 北京机电工程研究所, 北京 100074)

摘要: 提出了一种基于 *Q-learning* 的最优双中继节点选择方法。首先构建了基于社会意识的安全雾计算结构模型, 然后在该模型下设计了基于 *Q-learning* 算法的最优双中继节点选择方法, 实现了在动态环境下对最优双中继节点的选择, 最后对密钥生成速率、双中继节点选择速度和动态环境中双中继节点的选择准确率进行了分析。实验结果表明, 该方案能有效地在动态环境中选择最优双中继节点, 算法迅速收敛达到稳定, 最优中继节点选择速度得到有效提升。

关键词: *Q-learning*; 雾计算; 5G 网络; 社会意识; 物理层安全

中图分类号: TP393

文献标识码: A

doi: 10.11959/j.issn.1000-0801.2019176

Secure relay node selection method based on *Q-learning* for fog computing in 5G network

TU Shanshan^{1,2}, YU Jinliang^{1,2}, MENG Yuan^{1,2}, WAQAS M³, LIU Lei⁴

1. Faculty of Information Technology, Beijing University of Technology, Beijing 100124, China
2. Beijing Key Laboratory of Trusted Computing, Beijing 100124, China
3. Department of Electronics and Engineering, Tsinghua University, Beijing 100084, China
4. Beijing Electro-Mechanical Engineering Institute, Beijing 100074, China

Abstract: A *Q-learning*-based optimal dual-relay node selection method was proposed. Firstly, a security fog computing structure model based on social awareness was constructed, and then an optimal dual-relay node selection method based on *Q-learning* algorithm was designed under this model, which achieved the selection of optimal dual-relay nodes in dynamic environment. Finally, the key generation rate, the selection speed of dual-relay nodes and the selection accuracy of dual-relay nodes in dynamic environment were analyzed. The experimental results show that the scheme can effectively select the optimal dual-relay nodes in dynamic environment, the algorithm converges rapidly to a stable level, and the selection speed of the optimal relay node is effectively improved.

Key words: *Q-learning*, fog computing, 5G network, social awareness, physical layer security

收稿日期: 2019-06-01; 修回日期: 2019-07-01

通信作者: 涂山山, sstu@bjut.edu.cn

基金项目: 国家自然科学基金资助项目 (No.61801008); 国家重点研发计划经费资助项目 (No. 2018YFB0803600); 北京市自然科学基金资助项目 (No.L172049); 北京市教委科研计划经费资助项目 (No. KM201910005025)

Foundations Items: The National Natural Science Foundation of China (No.61801008), The National Key Research and Development Program of China (No. 2018YFB0803600), Beijing Natural Science Foundation (No.L172049), The Scientific Research Common Program of Beijing Municipal Commission of Education (No.KM201910005025)

1 引言

在过去的几年间, 移动网络流量的爆炸式增长反映出大众对于移动通信的需求越来越高^[1]。与此同时, 市场上也涌现了各式各样的移动应用, 这些应用在加重用户设备的计算负担的同时也提高了用户对于快速实时通信的要求。虽然云计算做到了前者, 但由于其地理位置远离用户, 因此无法满足低时延的网络需求^[2]。在这种情况下, 雾计算^[3-4]作为云计算概念的延伸应运而生, 它将云计算与网络边缘连接在一起。如今 5G 技术^[5]飞速发展, 雾计算与 5G 技术的结合^[6]可以达到降低用户延迟、提升系统性能的目的。雾计算是未来 5G 通信的关键技术, 有助于实现移动通信超低时延、高可靠、高能效的需求, 同时它可以利用设备直接传输链路来提高系统吞吐量, 解决了云计算移动性差、地理信息感知弱、时延高等问题^[7-8], 但是同时也带来了更重要的安全性问题。雾计算网络中不同终端用户之间的信任关系是构建相互协作环境以优化系统目标的必要条件。在移动雾计算网络中, 大量的移动终端用户通过无线网络与雾节点进行通信, 由于无线信号的开放性, 雾节点与终端节点之间的信任关系面临着众多的挑战, 如中间人攻击、窃听攻击等。目前, 在将传统安全技术应用于雾计算网络的研究中, 部分研究人员试图将云环境下的安全解决方案, 如云访问控制、密钥管理、数字签名、身份认证等应用在雾计算环境中, 但由于移动雾计算网络的多层结构以及终端在雾节点间的移动性, 使得移动终端密钥的在线分发、维护和管理变得异常困难^[9]。

由上所述, 近期研究学者利用物理层特性, 依靠信号处理、编码调制等方法为雾计算环境下用户的通信提供安全保障, 可以帮助移动终端用户与雾节点之间建立安全的传输链路。在无线物理层安全方面, 基于 Shannon^[10]提出的保密通信理论中利用物理层本质特征建立的加密机制得到

了大家的重视。受 Wyner^[11]的启发, Maurer^[12]提出了一种当窃听者的信道优于合法接收者时仍可以进行安全通信的方法, 该方法的核心是让通信双方共同产生一组安全密钥。相较于其他传统密码学密钥生成算法, 该方法节省了密钥分发的过程, 实现了基于密钥的物理层安全。物理层密钥是利用无线衰落信道的互易性和随机性生成的, 其本质是识别出依赖于收发信道介质的信道状态信息 (channel state information, CSI) 或接收信号强度 (receive signal strength, RSS) 的唯一性、连接源和目的等身份信息。在已有的研究中, Zeng^[13]概述了物理层密钥生成过程并讨论了实际挑战。Thai 等人^[14]提出了一种多天线合法节点物理层密钥生成方案。胡晓言等人^[15]在此基础上, 根据无线信号传播特性改进了算法, 使得算法具有更高的密钥生成速率。Tu 等人^[16]利用无线信号的 CSI 实现伪装攻击的入侵检测, 并引入了 Q-learning 算法, 提高了检测准确性。

随着社交网络的发展, 研究人员发现人们留在社交应用上的信息, 例如微信聊天、转账记录, 微博互动记录等, 拥有着重要的价值。在网络上一名用户与其他用户之间的交互数据可以抽象放映为该用户社交关系, 在一定程度上反映出用户在现实生活中的关系。比如人们在移动电话、短信业务和移动社交应用 (如微信、微博等) 上的互动频次可以在一定程度上反映出两者或远或近的关系。合理地运用社交网络的隐藏内涵可以用于提高现有雾计算网络的性能。在社会意识的应用方面, 有研究人员将社会意识与 D2D 网络相结合, 其研究的重点是如何利用 D2D 用户的社会特征来提高 D2D 的整体传输速率和资源利用率。Waqas 等人^[17]提出了一种具有社会意识的 D2D 安全通信系统, 合理地选择中继节点以提高物理层密钥生成速率。但目前还缺乏将社会意识与雾计算网络结合的研究。

综上所述, 本文针对雾环境下的物理层密钥



生成策略,将社会意识这一概念引入雾计算网络,并以此来解决雾计算目前遇到的易被监听等问题,提出了一种基于社会意识的安全密钥生成方法,本文的贡献如下。

- 构建了一种基于社会意识的雾计算结构模型,该模型将社会意识这一概念运用到雾计算环境中,在云节点与雾节点、雾节点与用户和云节点与用户之间建立物理链接和社会链接,满足了雾计算网络下各节点间安全通信的要求。
- 提出了一种基于 *Q-learning* 的双中继节点选择方法,实现了在动态的网络环境中双中继节点的实时选择,为实现“一次一密”的关键技术提供一种新的思路。
- 实验结果表明,基于 *Q-learning* 的双中继节点选择方法在区域内人数超过阈值时的选择速度较基于联合博弈的双中继节点选择方法更快,并且可以在动态的环境中选择最优的节点。

2 模型概述

2.1 系统模型

本文的系统模型如图1所示,此模型由3个

实体组成:云服务器、雾节点以及用户设备。在该模型中,云节点与雾节点之间通过有线网络连接,雾节点与终端用户节点之间通过无线网络进行通信,雾节点所在的雾层将云计算扩展到了网络边缘。雾节点是物联网系统中位置接近物联网边缘的设备,是对物联网终端进行数据预处理的单元,它为数据的存储、计算、传输、控制和管理提供了便利。该模型的各个实体表示为:云节点集合表示为 $M = \{1, 2, \dots, m\}, \forall m \in M$; 雾节点集合表示为 $N = \{1, 2, \dots, n\}, \forall n \in N$; 终端用户集合表示为 $L = \{1, 2, \dots, L\}, \forall L \in L$ 。

在实体与实体之间可以存在物理链接和社会链接。如存在物理链接表示节点间可以通过无线信号进行通信,存在社会链接则表示节点间具有较紧密的社会关系,节点能够被信任。本文使用 i_1, i_2 表示需要建立通信的两个节点,使用 j_1, j_2 表示两个中继节点, i_1, i_2, j_1, j_2 取值范围为 $\Omega = \{N, L\}$ 。本文用 $\alpha_{i_1, i_2, j_1, j_2}$ 来表示节点 i_1, i_2, j_1, j_2 之间是否存在物理链接,当 $\alpha_{i_1, i_2, j_1, j_2} = 1$ 时表示存在物理链接,反之 $\alpha_{i_1, i_2, j_1, j_2} = 0$ 时表示不存在物理链接;存在社会链接表示这两个实体存在较亲密的社会关系,即两实体可以互相信任,用 $\ell_{i_1, i_2, j_1, j_2}$ 来表示实体 i_1, i_2, j_1, j_2 之间是否存在社会链接,当

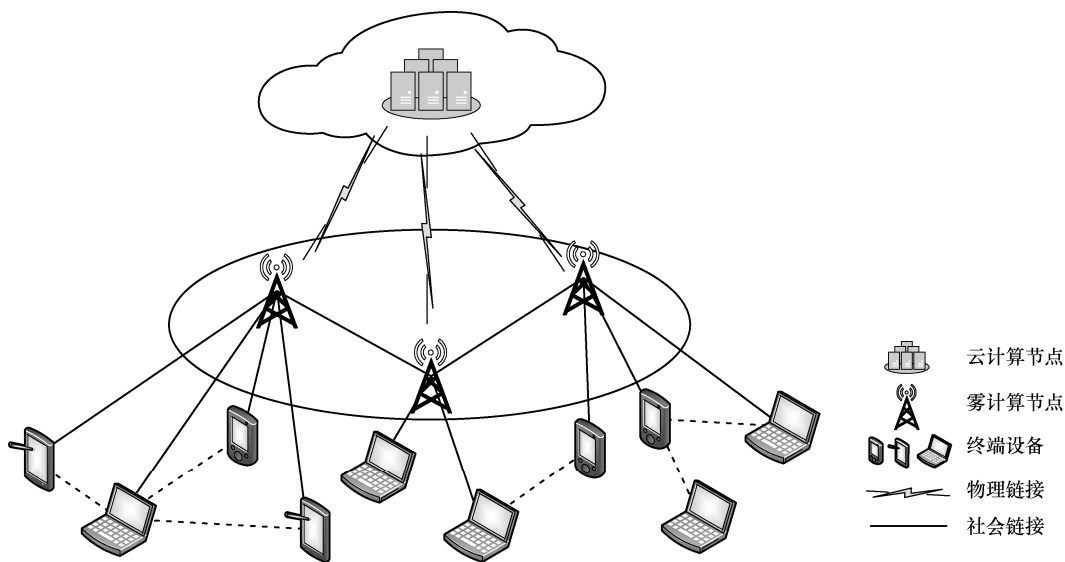


图1 基于社会意识的雾计算网络模型

$\ell_{i_1, i_2, j_1, j_2} = 2$ 时表示四者之间全部存在社会链接。

将雾计算网络中的通信分为以下 3 种模式：全信任(trusted)模式；不信任(untrusted)模式；混合(mixed)模式。3 种模式的判定条件可以总结为式 (1)：

$$\text{Mode} = \begin{cases} \{a_{i_1, i_2, j_1, j_2} = 1, \ell_{i_1, i_2, j_1, j_2} = 2\}, \text{trusted} \\ \{a_{i_1, i_2, j_1, j_2} = 1, \ell_{i_1, i_2, j_1, j_2} = 1\}, \text{untrusted} \\ \{a_{i_1, i_2, j_1, j_2} = 1, \ell_{i_1, i_2, j_1, j_2} = 0\}, \text{mixed} \end{cases} \quad (1)$$

2.2 密钥生成模型

针对不同的模式，其双中继密钥生成方法也不同，本文中使用的参考文献[17]所使用到的密钥生成模型，具体模型如图 2 所示。

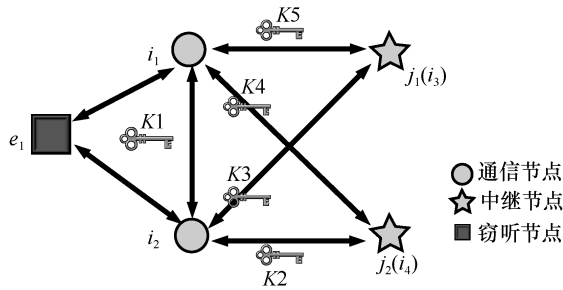


图 2 密钥生成模型

在 i_1 、 i_2 、 j_1 、 j_2 、 e_1 5 个点中， i_1 、 i_2 为需要建立通信的两个节点； j_1 、 j_2 为协助密钥生成的两个中继节点； e_1 为窃听节点，假设 e_1 和 i_1 、 i_2 的距离在半个波长以内。本文使用传统的物理层密钥生成方法，其方法可以概括为 3 个阶段。

(1) 接收端与发送端双方互相发送若干冲激信号并对接收到的信号进行量化。

(2) 提取一部分量化后的数据作为初始密钥。

(3) 接收端与发送端双方进行密钥协商，以确保量化过程中出错的数据被改正。在第一阶段中，第一时隙内 i_1 、 i_2 和 j_1 、 j_2 接收信号的估计信道增益 $\mathcal{H}_{1, i_1/i_2}$ 和 $\mathcal{H}_{1, i_1/i_2}$ 可用式 (2)、式 (3) 表示。

$$\mathcal{H}_{1, i_1/i_2} = g_i + \frac{X_{i_2/i_1}^*}{\|X_{i_2/i_1}\|^2} n_{i_2/i_1} \sim \mathcal{N}\left(0, \sigma_i^2 + \frac{\sigma_n^2}{\|X_{i_2/i_1}\|^2}\right) \quad (2)$$

$$\mathcal{H}_{1, i_1, j_2} = g_{i, j} + \frac{X_{j_1/j_2}^*}{\|X_{j_1/j_2}\|^2} n_{j_1/j_2} \sim \mathcal{N}\left(0, \sigma_i^2 + \frac{\sigma_n^2}{\|X_{i_2/i_1}\|^2}\right) \quad (3)$$

第二时隙内 i_1 、 i_2 处接收信号的估计信道增益 $\mathcal{H}_{2, i, j}$ 可用式 (4) 表示：

$$\mathcal{H}_{2, i, j} = g_{i, j} + \frac{X_j^*}{\|X_j\|^2} n_i \sim \mathcal{N}\left(0, \sigma_j^2 + \frac{\sigma_n^2}{\|X_j\|^2}\right) \quad (4)$$

其中， X_{j_1/j_2} 代表由 j_1/j_2 在密钥生成第一阶段传输的训练信号； X_{j_1/j_2}^* 则代表 X_{j_1/j_2} 的共轭； g_i 则代表通信节点传来信号的信道增益。

根据参考文献[17-18]相关部分的描述，在无中继节点协助生成密钥及有中继节点协助生成密钥的情况下，密钥生成速率分别为 $\mathcal{R}_{\text{direct}}$ 和 $\mathcal{R}_{\text{relay}}$ ，见式 (15)、式 (16)。

$$\mathcal{R}_{\text{direct}} = \frac{1}{T_c} I(\mathcal{H}_{1, i_1}; \mathcal{H}_{1, i_2}) = \frac{1}{T_c} \log\left(1 + \frac{\sigma_i^4 p^2 T_c^2}{4(\sigma_n^4 + \sigma_n^2 \sigma_i^2 p T_c)}\right) \quad (5)$$

$$\mathcal{R}_{\text{relay}} = \frac{1}{T_c} \left(I(\mathcal{H}_{1, i_1}; \mathcal{H}_{1, i_2}) + \sum_{i=1}^2 \sum_{j=1}^2 I(\mathcal{H}_{1, i, j}; \mathcal{H}_{2, i, j}) \right) = \frac{1}{T_c} \log\left(1 + \frac{\sigma_i^4 p^2 T_c^2}{8(2\sigma_n^4 + \sigma_n^2 \sigma_i^2 p T_c)}\right) \prod_{i=1}^2 \prod_{j=1}^2 \left(1 + \frac{\sigma_j^4 p^2 T_c^2}{8(\sigma_n^4 + \sigma_n^2 \sigma_j^2 p T_c)}\right) \quad (6)$$

其中，加性白噪声服从方差为 σ_n^2 的正态分布，通信节点的信道增益和中继节点的信道增益分别服从方差为 σ_i^2 、 σ_j^2 的正态分布； T_c^2 为 2.4 GHz 频段下的相干时间； p 为该网络中各节点间信号的发射功率。

当 $\mathcal{R}_{\text{relay}} > \mathcal{R}_{\text{direct}}$ 且 $\ell_{i_1, i_2, j_1, j_2} = 2$ 时，则有通信密钥 $\mathcal{K}$ 为：

$$\mathcal{K} = \begin{cases} \{K1, K2, K4\}, \text{sizeof}(K2, K4) < (K3, K5) \\ \{K1, K3, K5\}, \text{sizeof}(K2, K4) > (K3, K5) \end{cases} \quad (7)$$

当 $\mathcal{R}_{\text{relay}} > \mathcal{R}_{\text{direct}}$ 且 $\ell_{i_1, i_2, j_1, j_2} \neq 2$ 时，则有通信密



钥 $\mathcal{K}$ 为:

$$\mathcal{K} = \begin{cases} \{K1, K2 \oplus K4\}, \text{SIZEOF}(K2 \oplus K4) < (K3 \oplus K5) \\ \{K1, K3 \oplus K5\}, \text{SIZEOF}(K2 \oplus K4) > (K3 \oplus K5) \end{cases} \quad (8)$$

3 中继节点选择方法

本节将详细讲述基于 Q -learning 的双中继节点选择方法。 Q -learning 是一种可以在动态环境中

$$R = \begin{cases} \frac{1}{T_c} \text{lb} \left(\left(1 + \frac{\sigma_i^4 p^2 T_c^2}{8(2\sigma_n^4 + \sigma_n^2 \sigma_i^2 p T_c)} \right) \prod_{i=1}^2 \prod_{j=1}^2 \left(1 + \frac{\sigma_j^4 p^2 T_c^2}{8(\sigma_n^4 + \sigma_n^2 \sigma_i^2 p T_c)} \right) \right), \mathcal{R}_{\text{direct}} \leq \mathcal{R}_{\text{relay}} \\ \frac{1}{T_c} \text{lb} \left(1 + \frac{\sigma_i^4 p^2 T_c^2}{4(\sigma_n^4 + \sigma_n^2 \sigma_i^2 p T_c)} \right), \mathcal{R}_{\text{direct}} > \mathcal{R}_{\text{relay}} \end{cases} \quad (11)$$

在本文中, Agent 在选择动作时采用 ε -greedy 策略, 即在 ε 概率下 Agent 会将当前 Q 表中 Q 值最高的动作作为下一动作, 在 $1-\varepsilon$ 的概率下随机选择一个动作而不考虑当前状态与收益。 Q 值更新见式 (12):

$$Q(S_t, A_t) \leftarrow Q(S_t, A_t) + \alpha(R + \gamma \max_{A'} Q(S'_{t+1}, A'_{t+1}) - Q(S_t, A_t)) \quad (12)$$

其中, $Q(S_t, A_t)$ 为在 S_t 状态下选择动作 A_t 的 Q 值。 α 为学习效率, 其值越大, 学习速度越快, 保留记忆中的效果就越少; 相反, 其值越小, 学习速度越慢, 保留记忆中的效果就越多。 γ 为折扣因子, 其值越大, 记忆中的利益 $\max Q(S'_{t+1}, A'_{t+1})$ 在新 Q 值中所占比重就越大, Agent 就越重视以往的经验; 相反其值越小 Agent 就越重视眼前的利益 R 。

基于 Q -learning 的双中继节点选择方法如算法 1。

算法 1 Q -learning 的双中继节点选择方法

步骤 1 初始化

初始化 $Q(S_t, A_t) = 0$

初始化节点间物理链接状态 $P(a, b), a \in (1, 2, 3, \dots, N), b \in (1, 2, 3, \dots, \mathcal{L})$

利用不充分条件找到最优解的强化学习算法。在本文中, 设定状态 S 为潜在中继节点 j_1, j_2 的集合; 动作 A 为潜在中继节点 j_1, j_2 的集合; 奖励函数矩阵 R 为对于当前选定的 i_1, i_2 , 使用 j_1, j_2 中继节点之后的密钥生成速率; 其中, N 为候选节点个数, 具体见式 (9) ~ 式 (11)。

$$S_t = \{r_1, r_2, r_3, \dots, r_t\}, t \in \{1, 2, 3, \dots, N\} \quad (9)$$

$$A_t = \{r_1, r_2, r_3, \dots, r_t\}, t \in \{1, 2, 3, \dots, N\} \quad (10)$$

初始化节点间社会关系状态 $S(a, b), a, b \in (1, 2, 3, \dots, \mathcal{L})$

随机选择需要建立的雾节点和终端设备 i_1, i_2

根据物理链接状态 P 和社会关系状态 S 选择候选节点组合 J_{node}

步骤 2 根据当前状态选择动作

根据 ε -greedy 策略选择动作 A_t

估算动作 A_t 带来的收益 R

根据式 (11) 更新 $Q(S_t, A_t)$

更新当前状态 S_t 为 S_{t+1}

循环执行步骤 2, 直至执行 n 次

步骤 3 返回结果

当需要新节点组合时

返回动作 A_t 所对应的节点组合即最优双中继节点

4 性能分析

在仿真实验中, 本文假设实验环境在面积为 $100 \text{ m} \times 100 \text{ m}$ 的一块区域中有若干个雾节点。雾节点周围散布着若干终端设备, 这些终端设备可以是通信节点也可以是中继节点。雾节点与终端设备在通信时发射功率为 100 dBm , 信号频率为 2.4 GHz ,

区域内大部分设备都可以与雾节点相连接,并且随机设定每对终端和用户之间是否存在社会关系。

4.1 密钥生成速率分析

如图3所示,在本方法中,密钥生成速率随着设备节点数量的增加而增加。这是由于当区域内设备节点的数量增加时,通信节点能够选择的候选中继节点更多,因此,与区域内只有较少设备节点时相比,通信节点较易选择到最优节点组合。当通信节点与所选择的中继节点组合处于信任模式时,即 $\{\ell_{i_1, i_2, j_1, j_2} = 2\}$, 密钥生成速率高于其处在非信任模式或混合模式下,即 $\{\ell_{i_1, i_2, j_1, j_2} = 1\}$ 或 $\{\ell_{i_1, i_2, j_1, j_2} = 0\}$ 。这是由于在物理层密钥生成的量化过程中,密钥生成速率取决于量化因子 μ , 见式(13):

$$\mu = \frac{1}{2R_{ij}} e^{-1/\text{SNR}} \quad (13)$$

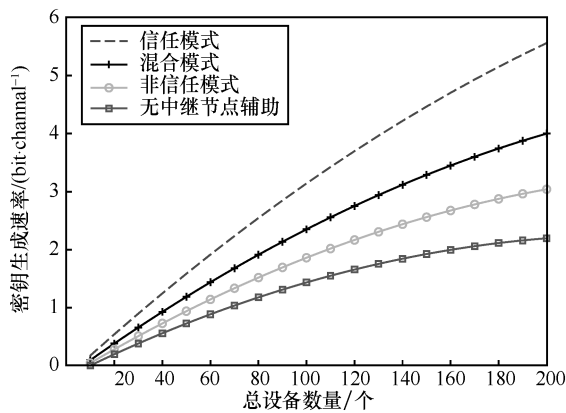


图3 不同总设备数量下各种模式的密钥生成速率对比

量化因子 μ 的取值由信道互易性 $R_{i,j}$ 和信噪比SNR决定^[19], $R_{i,j}$ 与SNR相关,当通信节点与辅助节点处于信任模式时,它们可以获得更高的信道互易性和信噪比,从而获得更高的密钥生成速率。在本实验中,信任模式下密钥生成速率比混合模式下密钥生成速率平均高出32%,比非信任模式下高出77%,比不使用中继节点辅助时平均高出153%。

总之,选择合适的中继节点辅助密钥生成过

程可以有效地提高密钥生成率,并且当具有足够多的相互信任且愿意相互合作的节点时,密钥生成速率会更贴近理论上限。

4.2 选择方法速度分析

如图4所示,将本方法与参考文献[17]中基于联合博弈的双中继节点选择方法和基于参考文献[20]中DQL算法的双中继节点选择方法对比,在节点较少时基于联合博弈论的方法更有效;在节点较多时基于Q-learning的方法更有效,且随着节点数的增加,基于Q-learning的方法比基于联合博弈论选择最优中继节点的方法具有更高的时间增长率。这是由于Q-learning算法在训练过程中逐步逼近最优解。当区域内设备数量较少时,直接比较各个组合的收益并选择中继节点所需要的时间小于训练过程所需要花费的时间。因此基于联合博弈论选择中继节点的方法中花费的时间小于基于Q-learning的方法花费的时间。并且,参考文献[17]选择中继节点的方法所需要的时间与区域内设备节点数量关系呈线性,而基于Q-learning的方法所需时间呈二次性,这是因为随着区域内设备数量的增加,Q-learning算法需要维护的Q表大小增长得越来越快,所需时间也随之增加。实验表明,当区域内总设备数量较少时,基于联合博弈论选择中继节点的方法所需时间略小于基于Q-learning的中继节点选择方法,当区域内总设备数量较大时,参考文献[17]选择中继节点的方法与基于Q-learning的方法花费的时间相差越来越大。在多次实验中,基于DQL的方法与本方法的结果近似。

总之,基于Q-learning的中继选择方法在选择速度方面比参考文献[15]中的方法略低,并且所需时间随区域内设备数量的增长而增长。

4.3 动态选择特性分析

本文考虑了节点之间通信受环境影响的问题,比如人员的移动、环境干扰或作为中继节点的设备突然断电下线等,这些问题造成了已选择的中

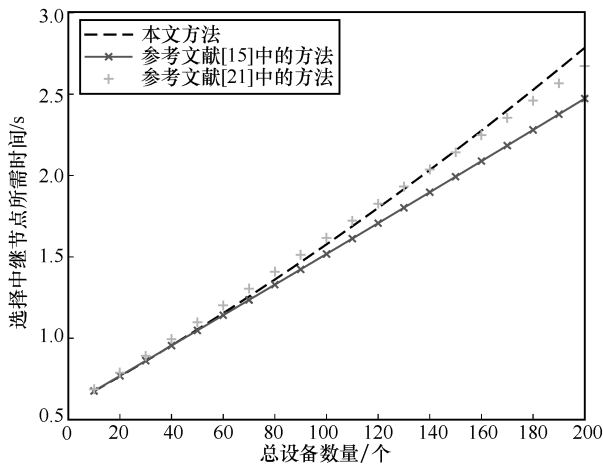


图4 不同总设备数量下各方法选择最优中继节点所需的时间

继节点无法继续为通信节点提高密钥生成率。在这种情况下,重新计算所有可能节点组合的收益并选择双中继节点会大大降低系统的性能。本文提出的方法可以有效地减少再次选择中继节点所花费的时间,从而减少了“一次一密”中密钥生成过程的时间。

本实验中,取环境变化率作为 x 轴,取区域内设备数量作为 y 轴,分别以重新选择时间和选择准确率作为 y 轴对本方法的动态性能进行检验,同时将区域内总设备数量保持在 200 个。用户变化率是指模拟设备由于移动等特殊原因,不再适合作为中继节点辅助通信节点生成密钥时的环境变化情况。环境变化率用来衡量区域内设备的变化幅度,比如当环境变化率为 5% 时,代表区域内环境与上一时刻相比变化不大,通信节点仍然可以选择当前中继节点组合辅助生成密钥。

如图 5 所示,当环境变化率逐渐增加时,重新选择时间也逐渐增长。但在任意环境变化率下,本方法都比基于联合博弈论的方法需要的时间更短。基于 Q -learning 中继节点选择方法比参考文献[17]中的方法重新选择花费的时间平均少 53%。这是由于 Q -learning 算法是面向动态环境的强化学习算法。当区域内设备数量较多时,基于联合博弈论的方法在重新选择中继节点时需要将每一种可能组合都重新遍历一次,这耗费了大量的时

间。而 Q -learning 算法可以根据策略训练 Agent,在得到的 Q 表中做出细微的调整,进而适应变化的环境,当需要选择新的中继节点组合时及时获取当前环境下的最优组合。本方法准确率如图 6 所示,在区域内节点总数量为 200 时,在不同程度的用户变化下,3 种方法的准确率均在 90% 以上,其中基于 Q -learning 中继节点选择方法略低于参考文献[17]中的方法,在用户变化率达到 100% 时,基于 Q -learning 中继节点选择方法的准确率比参考文献[17]中的方法准确率平均低 1%。由于 DQL 中两个 Q 表交替更新,并没有增大实际计算量,所以基于 DQL 的方法与基于 Q -learning 的中继节点选择方法表现相近。

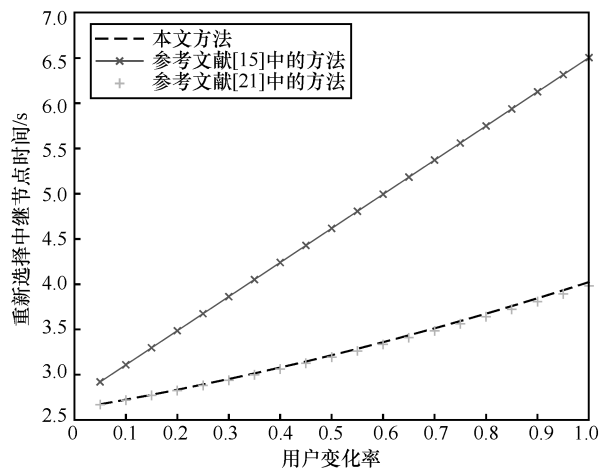


图5 不同用户变化率下各选择方法的重新选择最优中继节点所需的时间

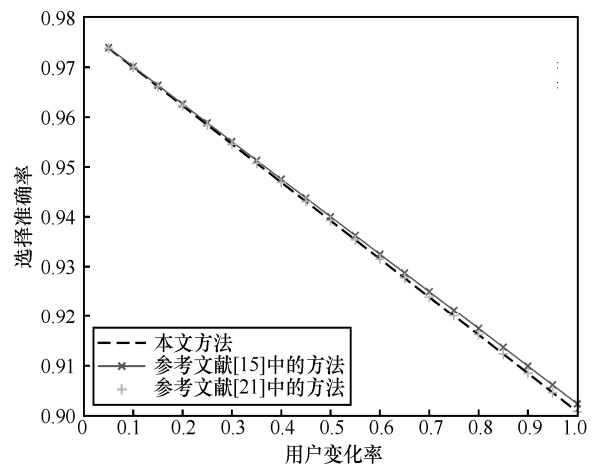


图6 不同用户变化率下各选择方法的选择准确率

综上所述,在动态环境中,基于 Q -learning 中继节点选择方法比参考文献[17]中的方法更适应环境的变化。基于 DQL 的方法与基于 Q -learning 中继节点的方法相比,去除了 Q 值估计过大的干扰,从而使得准确率有所提升。

5 结束语

本文分析了在与 5G 技术结合的移动雾计算网络中物理层密钥生成策略存在的问题,引入了社会意识的概念,并提出了一种利用雾计算网络中各实体之间的无线信道特性选择最优双中继节点的方法,从而提高密钥生成速率。本文首先建立了基于社会意识的雾计算网络模型,并在该模型的基础上设计了一种基于 Q -learning 的安全最优双中继节点选择方法,该方法在包含大量设备的环境中可以动态实时地选择最优双中继节点,从而获得较高的密钥生成速率。仿真实验结果表明,该方法能有效地在动态环境中选择最优双中继节点,算法迅速收敛并达到稳定,具有较高的精度。在接下来的工作中,将探讨基于社会意识的雾计算网络中雾计算节点与云计算节点之间的安全通信实现方式。

参考文献:

- [1] Cisco. Cisco delivers vision of fog computing to accelerate value from billions of connected devices[R]. 2017.
- [2] SARKAR S, CHATTERJEE S, MISRA S. Assessment of the suitability of fog computing in the context of internet of things[J]. IEEE Transactions on Cloud Computing, 2018, 6(1): 46-59.
- [3] ALRAWAIS A, ALHOTHAILY A, HU C, et al. Fog computing for the internet of things: security and privacy issues[J]. IEEE Internet Computing, 2017, 21(2): 34-42.
- [4] CHAUDHARY R, KUMAR N, ZEADALLY S. Network service chaining in fog and cloud computing for the 5G environment: data management and security challenges[J]. IEEE Communications Magazine, 2017, 55(11): 114-122.
- [5] 王庆扬, 谢沛荣, 熊尚坤. 5G 关键技术与标准综述[J]. 电信科学, 2017, 33(11): 112-122.
WANG Q Y, XIE P R, XIONG S K. Key technology and standardization progress for 5G[J]. Telecommunications Science, 2017, 33(11): 112-122.
- [6] 朱雪田, 夏旭, 齐飞. 5G 网络关键技术和业务[J]. 电子技术应用, 2018, 44(9): 1-4.
ZHU X T, XIA X, QI F. 5G key technologies and business forecast[J]. Application of Electronic Technique, 2018, 44(9): 1-4.
- [7] BOTTA A, DONATO W D, PERSICO V, et al. Integration of cloud computing and internet of things: a survey[J]. Future Generation Computer Systems, 2016, 56(1): 684-700.
- [8] SINGH S P, NAYYAR A, KUMAR R, et al. Fog computing: from architecture to edge computing and big data processing[J]. The Journal of Supercomputing, 2019, 75(4): 2070-2105.
- [9] MA Z, XIE J, LI H, et al. The role of data analysis in the development of intelligent energy networks[J]. IEEE Network, 2017, 31(5): 88-95.
- [10] SHANNON C E. Communication theory of secrecy systems [J]. Bell System Technical Journal, 1949, 28(4): 656-715.
- [11] WYNER A D. The wire-tap channel[J]. Bell System Technical Journal, 1975, 54(8): 1355-1387.
- [12] MAURER U M. Secret key agreement by public discussion from common information[J]. IEEE Transactions on Information Theory, 1993, 39(3): 733-742.
- [13] ZENG K. Physical layer key generation in wireless networks: challenges and opportunities[J]. IEEE Communications Magazine, 2015, 53(6): 33-39.
- [14] THAI C D T, LEE J, TONY Q S, et al. Physical-layer secret key generation with colluding untrusted relays[J]. IEEE Transactions on Wireless Communications, 2016, 15(2): 1517-1530.
- [15] 胡晓言, 金梁, 黄开枝, 等. 基于信号传播特性的物理层密钥生成方案[J]. 电子学报, 2019, 47(2): 483-488.
HU X Y, JIN L, HUANG K Z, et al. Physical layer secret key generation scheme based on signal propagation characteristics[J]. ACTA Electronica Sinica, 2019, 47(2): 483-488.
- [16] TU S, WAQAS M, REHMAN S U, et al. Security in fog computing: a novel technique to tackle an impersonation attack[J]. IEEE Access, 2018(6): 74993-75001.
- [17] WAQAS M, AHMED M, LI Y, et al. Social-aware secret key generation for secure device-to-device communication via trusted and non-trusted relays[J]. IEEE Transactions on Wireless Communications, 2018, 17(6): 3918-3930.
- [18] AHLWEDE R, CSISZÁR I. Common randomness in information theory and cryptography. Part I: secret sharing[J]. IEEE Transactions on Information Theory, 1993, 39(4): 1121-1132.
- [19] 张启星, 付敬奇. 基于信道特征提取的物理层安全密钥生成方法[J]. 电子测量与仪器学报, 2019, 33(1): 16-22.
ZHANG Q X, FU J Q. Physical layer secure key generation method based on channel feature extraction[J]. Journal of Electronic Measurement and Instrumentation, 2019, 33(1): 16-22.
- [20] 孟远, 涂山山, 于金亮. 雾计算中基于 DQL 算法的伪装攻击检测方案[J]. 计算机工程与应用, 2019(已录用).



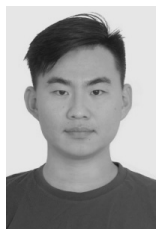
MENG Y, TU S S, YU J L. Detection scheme of camouflage attack based on DQL algorithms in fog computing[J]. Computer Engineering and Applications, 2019(accepted).

- [21] MNIH V, KAVUKCUOGLU K, SILVER D, et al. Human-level control through deep reinforcement learning[J]. Nature, 2015, 518(7540): 529-533.

[作者简介]



涂山山（1983- ），男，北京工业大学信息学部、可信计算北京市重点实验室副教授、硕士生导师，主要研究方向为云计算、MEC、信息安全技术。



于金亮（1996- ），男，北京工业大学信息学部、可信计算北京市重点实验室硕士生，主要研究方向为雾计算、机器学习、信息安全技术。



孟远（1995- ），男，北京工业大学信息学部、可信计算北京市重点实验室硕士生，主要研究方向为雾计算、强化学习、信息安全技术。



WAQAS M（1985- ），男，清华大学电子工程系博士生，主要研究方向为 5G 网络、MEC、信息安全技术。



刘雷（1982- ），男，北京机电工程研究所高级工程师，主要研究方向为航空电子、机电、机器人和智能系统。